IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MISSOURI

Melanie Burns, *individually and on behalf of all others similarly situated*, Plaintiff, v. Navvis & Company, LLC d/b/a Navvis, Defendant.	Case No. 4:24-cv-00039 **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Melanie Burns ("Plaintiff"), individually and on behalf of all others similarly situated (the "Class" or "Class Members"), brings this Class Action Complaint (the "Complaint") against Defendant Navvis & Company, LLC, d/b/a Navvis ("Defendant"). The allegations set forth in this Complaint are based on the personal knowledge of the Plaintiff and upon information and belief and further investigation of counsel.

I. NATURE OF THE ACTION

1. This is a data breach class action against Defendant for its failure to adequately secure and safeguard confidential and sensitive information held throughout the typical course of business of Plaintiff and the Class.

2. Over the course of two days – occurring on or about July 12 and July 25, 2023 – an unauthorized third party actor gained access to the Defendant's network and computer systems and obtained unauthorized access to Defendant's files (the "Data Breach").

3. Upon information and belief, thousands of individuals and their information was affected in the Data Breach. Defendant has not yet disclosed the exact number of individuals impacted by the Data Breach. The information exposed or otherwise accessed by an authorized

third-party in the Data Breach included Plaintiffs' and the Classes' personal identifying information and protected health information, including names, dates of birth, Bene Hic numbers, medical dates of service, and patient account numbers (collectively, "PII/PHI").

4. Defendant learned of the Data Breach on or about July 25, 2023.

5. After learning of the incident, Defendant conducted an investigation and engaged outside cybersecurity professionals and data privacy counsel. Defendant, so far, has yet to inform affected individuals when it completed its investigation or when it completely learned of the extent of the Data Breach.

6. On or about December 29, 2023, Defendant notified affected individuals that their PII/PHI was impacted in the Data Breach. Although Defendant learned of the Data Breach in July 2023, it waited over five (5) months to notify affected individuals of the Data Breach.

7. Defendant had numerous statutory, regulatory, contractual, and common law duties and obligations, including those based on its affirmative representations to Plaintiff and the Class, to keep their PII/PHI confidential, safe, secure, and protected from unauthorized disclosure or access.

8. Plaintiff and the Class have taken reasonable steps to maintain the confidentiality and security of their PII/PHI.

9. Plaintiff and the Class reasonably expected Defendant to keep their PII/PHI confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

10. Defendant, however, breached its numerous duties and obligations by failing to implement and maintain reasonable safeguards; failing to comply with industry-standard data security practices and federal and state laws and regulations governing data security; failing to

properly train its employees on data security measures and protocols; failing to timely recognize and detect unauthorized third parties accessing its system and that substantial amounts of data had been compromised; and failing to timely notify the impacted Class.

11. In this day and age of regular and consistent data security attacks and data breaches, in particular in the financial industries, and given the sensitivity of the data entrusted to Defendant, this Data Breach is particularly egregious and foreseeable.

12. By implementing and maintaining reasonable safeguards and complying with standard data security practices, Defendant could have prevented this Data Breach.

13. Plaintiff and the Class are now faced with a present and imminent lifetime risk of identity theft or fraud. These risks are made all the more substantial, and significant because of the inclusion of their PII/PHI.

14. PII/PHI has great value to cyber criminals. As a direct cause of Defendant's Data Breach, Plaintiff's and the Class Members' PII/PHI is in the hands of cyber-criminals and may be available for sale on the dark web for other criminals to access and abuse at the expense of Plaintiff and the Class. Plaintiff and the Class face a current and lifetime risk of identity theft or fraud as a direct result of the Data Breach.

15. Upon information and belief, Defendant acknowledges the imminent threat the Data Breach has caused to Plaintiff.

16. The modern cyber-criminal can use the PII/PHI and other information stolen in cyber-attacks to assume a victim's identity when carrying out various crimes such as:

a. Obtaining and using a victim's credit history;

b. Making financial transactions on their behalf and without their knowledge or consent, including opening credit accounts in their name or taking out loans;

c. Impersonating them in written communications, including mail e-mail and/or text messaging;

d. Stealing, applying for and/or using benefits intended for the victim;

e. Committing illegal acts while impersonating their victim which, in turn, could incriminate the victim and lead to other legal ramifications.

17. Plaintiff's and Class's PII/PHI was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect Plaintiff's and Class's PII/PHI. Defendant not only failed to prevent the Data Breach, but after discovering the Data Breach in July 2023, Defendant waited until on or around December 29, 2023 to notify state Attorney Generals, and to affected individuals such as Plaintiff and members of the Class.

18. As a result of Defendant's delayed response to the data breach, Plaintiff and the Class had no idea their PII/PHI had been compromised, and that they were, and continue to be, at significant and imminent risk of identity theft, fraud and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes because of Defendant's negligence.

19. Plaintiff brings this action on behalf of all persons whose PII/PHI was compromised in the Data Breach as a direct consequence for Defendants failure to:

(i) adequately protect consumers' PII/PHI entrusted to it,

(ii) warn its current and former customers, as well as potential customers of their inadequate information security practices, and

(iii) effectively monitor their websites and platforms for security vulnerabilities and incidents.

20. Defendant's conduct amounts to negligence and violates federal and state statutes

and guidelines.

21. As a result of the Data Breach, Plaintiff and the Class suffered ascertainable losses, including but not limited to, a loss of privacy. These injuries include:

(i) the invasion of privacy;

(ii) the compromise, disclosure, theft, and imminent unauthorized use of Plaintiff's and the Class's PII/PHI;

(iii) emotional distress, fear, anxiety, nuisance and annoyance related to the theft and compromise of their PII/PHI;

(iv) lost or diminished inherent value of PII/PHI;

(v) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII/PHI; lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time or wages;

(vi) the continued and increased risk to their PII/PHI, which, (a) remains available on the dark web for individuals to access and abuse; and (b) remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII/PHI of Plaintiff and the Class.

22. Plaintiff seeks to remedy these harms and prevent any future data compromise on behalf of herself and all similarly situated persons whose PII/PHI was compromised and stolen as a result of the Data Breach and remains at risk due to inadequate data security practices employed

by Defendant.

23. Accordingly, Plaintiff, on behalf of herself and the Class, asserts the claims alleged below. Plaintiff also seeks injunctive relief, declaratory relief, monetary damages, and all other relief as authorized in equity by law, or any other relief the Court deems just and appropriate.

II. PARTIES

24. Plaintiff Melanie Burns is, and at all relevant times was, a citizen of Oklahoma City, Oklahoma. Plaintiff received Defendant's Notice of Data Breach letter (the "Notice") on or about December 29, 2023 from Defendant over five (5) months after Defendant learned of the Data Breach. *See*, **Exhibit 1** (Redacted Copy of the Notice of Data Breach to Melanie Burns.)

25. The Notice advised Plaintiff that the PII/PHI that could have been accessed included her personal information and medical treatment information including but not limited to her name, date of birth, Bene Hic number, medical date of service, and patient account number.

26. Prior to this Data Breach, Plaintiff had taken steps to protect and safeguard her PII/PHI including monitoring her PII/PHI closely. She has not knowingly transmitted her PII/PHI over unsecured or unencrypted internet connections.

27. Plaintiff has suffered actual damages and is at imminent, impending, and substantial risk for identity theft and future economic harm due to the highly sensitive nature of the information that was targeted and stolen in the Data Breach. Since learning about the breach Plaintiff has taken the *necessary* preventative measures in an effort to mitigate the risk of any potential instances of identity theft of fraud, to review financial statements and identity theft protection reports to preemptively detect and deter actual instances of identity theft or fraud. Plaintiff has suffered and continues to suffer emotional anguish and distress, including but not limited to fear and anxiety related to the data theft and compromise of her PII/PHI. Plaintiff will

continue to spend additional time and incur future economic costs associated with the detection and prevention of identity theft or fraud.

28. Defendant creates and manages electronic data management software used by health plans, systems, facilities, and professionals to store or transmit PII/PHI.

29. Defendant's principal place of business is located at 555 Maryville University Drive, Suite 240, St. Louis, MO 63141.

30. Defendant collected and continues to collect the PII/PHI of its customers and clients throughout its usual course of business operations.

31. Defendant's privacy policy "recognizes that the privacy of… personal information is important…."[1] Defendant only shares PII/PHI with "third parties who perform functions or services on our behalf as outlined in this Privacy Policy and otherwise as permitted by law."[2]

32. By obtaining, collecting, using, and deriving benefit from Plaintiff's and Class's PII/PHI, Defendant assumed legal and equitable duties to those persons, and knew or should have known that it was responsible for protecting Plaintiff's and Class's PII/PHI from unauthorized disclosure and/or criminal cyber activity.

III. JURISDICTION AND VENUE

33. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d), *et seq*. The amount in controversy exceeds $5 million, exclusive of interest and costs. There are more than 100 members in the proposed Class, and at least one member of the Class is a citizen of a state different from Defendant. Thus, minimal diversity exists

[1]https://www.navvishealthcare.com/legal/#:~:text=We%20collect%20and%20may%20use,services%20and%20to%20improve%20the

[2] *Id*.

under 28 U.S.C. § 1332(d)(2)(A).

34. This Court has personal jurisdiction over Defendant because Defendant's principal places of business is located within this District and the Defendant conducts substantial business in this district.

35. Venue is proper in this Court under 28 U.S.C. § 1391, because a substantial part of the events or omissions giving rise to these claims occurred in, were directed to, and/or emanated from this District, and Defendant resides within this judicial district.

IV. FACTUAL ALLEGATIONS

A. Background

36. In the ordinary course of its business practices, Defendant stores, maintains, and uses Plaintiff's and Class Members' PII/PHI, which includes but is not limited to information such as:

a. Names; and

b. Medical treatment information.

37. Defendant understands the importance of securely storing and maintaining PII/PHI.

B. The Data Breach

38. Defendant became aware of the Data Breach on or about July 25, 2023.

39. Defendant then took steps to secure its systems and network including retaining independent cybersecurity experts to investigate the matter further, but neglected to quickly and appropriately notify affected individuals of the Data Breach until on or about December 29, 2023.

40. Defendant waited over five (5) months after learning of the Data Breach before notifying all affected individuals, including Plaintiff and Class Members.

41. Additionally, though Plaintiff and the Class have an interest in ensuring that their

information remains protected, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures taken by Defendant to ensure a data breach does not occur again have not been shared with regulators, Plaintiff or Members of the Class.

C. Defendant Was Aware of the Data Breach Risks

42. In light of recent high-profile data breaches at other companies in the healthcare industry, Defendant knew or should have known that their electronic records would be targeted by cybercriminals.

43. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive. . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[3]

44. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[4]

45. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

46. Defendant had and continues to have obligations created by implied contract, industry standards, common law, and representations made to Plaintiff and the Class, to keep their PII/PHI private and confidential and to protect it from unauthorized access, disclosure or exfiltration.

---

[3] *FBI, Secret Service Warn of Targeted*, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited June 23, 2021).

[4] *See* Maria Henriquez, Iowa City Hospital Suffers PII/PHI shing Attack, Security Magazine (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-PII/PHI shing-attack (last visited Aug. 24, 2021).

47. Plaintiff and the Class provided their PII/PHI to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with their obligations to employ reasonable care to keep such information confidential and secure from unauthorized access.

48. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and data breaches in the banking, credit, and financial service industries preceding the date of the Data Breach.

49. Indeed, data breaches, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known and foreseeable to the public and to anyone in Defendant's industry, including Defendant.

50. According to the Federal Trade Commission ("FTC"), identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take substantial time, money, and patience to resolve.[5] Identity thieves use the stolen PII/PHI for a variety of crimes, including but not limited to, credit card fraud, telephone or utilities fraud, and bank and finance fraud.[6]

51. The PII/PHI of Plaintiff and the Class were accessed and taken by cyber criminals

---

[5] *See Taking Charge, What to Do If Your Identity is Stolen*, FTC, 3 (Apr. 2013), https://www.myoccu.org/sites/default/files/pdf/taking-charge-1.pdf (last visited Nov. 24, 2021).

[6] *Id*. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id*.

for the very purpose of engaging in illegal and unethical conduct, including crimes involving identity theft, fraud, or to otherwise profit by selling their data to other criminals who purchase PII/PHI for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

52. Defendant knew, or should have known, the importance of safeguarding the PII/PHI of Plaintiff and the Class and of the foreseeable consequences that would occur if Defendant's data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class as a result of a breach.

53. Plaintiff and the Class now face years of constant monitoring and surveillance of their financial and personal records. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII/PHI as a direct result of the Data Breach.

54. The injuries to Plaintiff and Class were directly and proximately caused by Defendant's own failure to install, implement or maintain adequate data security measures, software and other industry best practices for safeguarding the PII/PHI of Plaintiff and the Class.

D. Defendant Failed to Comply with FTC Guidelines

55. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable and adequate data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

56. In 2022, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their networks' vulnerabilities; and implement policies to correct any

security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[7]

57. The FTC further recommends that companies not maintain PII/PHI longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

58. The FTC has brought enforcement actions against businesses for failing to protect consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

59. Defendant failed to properly implement basic data security practices, and its failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII/PHI constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

60. To prevent and detect cyber attacks, including the cyber attack on Defendants network that resulted in the Data Breach, Defendant could and should have implemented, as

[7] Ritchie, J. N. & A., & Jayanti, S.F.-T. and A. (2022, April 26). *Protecting personal information: A guide for business.* Federal Trade Commission. https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last accessed October 27, 2023)

recommended by the United States Government and FTC, the following measures:

a. Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of malware and how it is delivered;

b. Enable strong spam filters to prevent PII/PHI shing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing;

c. Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users;

d. Configure firewalls to block access to known malicious IP addresses;

e. Patch operating systems, software, and firmware on devices using a centralized patch management system;

f. Set anti-virus and anti-malware programs to automatically conduct regular scans and/or repairs;

g. Create and manage the use of privileged accounts based on the varying level of accessibility using a principle of least privilege: wherein no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary, such as any internal IT employees;

h. Configure access controls—including file, directory, and network share permissions— with least privilege in mind. If a user only needs to read

specific files, the user should not have write access to those files, directories, or shares;

i. Disable macro scripts from Microsoft Office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications;

j. Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common malware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder;

k. Consider disabling Remote Desktop protocol (RDP) if it is not being used;

l. Use application whitelisting, which only allows systems to execute programs known and permitted by security policy;

m. Execute operating system environments or specific programs in a virtualized environment; and

n. Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

61. Defendant was at all times fully aware of its obligation to protect the PII/PHI of former customers, current customers, and prospective customers. Defendant was also aware of the significant repercussions that would result from its failure to do so.

E. Defendant Failed to Comply with Industry Standards

62. A number of industry and national best practices have been published and should have been used as a go-to resource and authoritative guide when developing Defendant's

cybersecurity practices. Best cybersecurity practices that are standard in the financial services industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

63. Upon information and belief, Defendant failed to meet the minimum standards of the following cybersecurity frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established standards in reasonable cybersecurity readiness. These frameworks are existing and applicable industry standards in Defendant's industry, and Defendant failed to comply with these accepted standards, thereby opening the door to the cyber-attack and causing the Data Breach.

64. The occurrence of the Data Breach is indicative that Defendant failed to adequately implement one or more of the above measures to prevent or circumvent ransomware attacks or other forms of malicious cybercrimes, resulting in the Data Breach.

F. Personally Identifiable Information and Protected Health Information Holds Value to Cyber Criminals

65. Businesses, such as Defendant, that store PII/PHI in their daily course of business are more likely to be targeted by cyber criminals. Credit card, routing, bank account and other financial numbers are highly sought data targets for hackers, but the PII/PHI involved in the Data Breach is desirable to cyber criminals, as it can be easily used to perpetrate acts of identity theft

and other types of fraud.

66. The PII/PHI of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web to obtain PII/PHI of other unknown individuals. Numerous sources cite dark web pricing for stolen identity credentials. For example, PII/PHI can be sold at a price ranging from $40 to $200, and banking details have a price range of $50 to $200.[8]

67. The unauthorized access by cyber criminals left them with the tools to perform the most thorough identity theft—they have obtained all the essential PII/PHI that can be used to mimic the identity of the victim. The PII/PHI of Plaintiff and the Class stolen in the Data Breach constitutes a dream for hackers or cyber criminals and a nightmare for Plaintiff and the Class. Stolen personal data of Plaintiff and the Class represents essentially one-stop shopping for identity thieves indefinitely.

68. The FTC has released its updated publication on protecting PII/PHI for businesses, which includes instructions on protecting PII/PHI, properly disposing of PII/PHI, understanding network vulnerabilities, implementing policies to correct security problems, using intrusion detection programs, monitoring data traffic, and having in place a response plan.

69. General policy reasons support such an approach. A person whose personal information has been compromised may not see any signs of identity theft for years. According to the United States Government Accountability Office ("GAO") Report to Congressional Requesters:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years.

[8] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web- how-much-it-costs (last visited Apr. 7, 2021).

> As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[9]

70. Companies recognize that PII/PHI is a valuable asset and a valuable commodity, but also necessary throughout the typical course of business with consumers.

71. Identity thieves may commit various types of crimes such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, and/or using the victim's information to obtain a fraudulent tax refund or fraudulent unemployment benefits. The United States government and privacy experts acknowledge that it may take years for identity theft to come to light and be detected.

72. Criminals can, for example, use PII/PHI to create false bank accounts or file fraudulent tax returns or other tax related forms and documents using an alias of their victim. Class members whose PII/PHI has been compromised in the Data Breach now face a real, present, imminent, and substantial risk of identity theft and other problems associated with the disclosure of their PII/PHI and will need to monitor their credit and tax filings for an indefinite duration.

73. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, because those victims can file disputes, cancel or close credit and debit cards and/or accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not nearly impossible, to change.

74. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the

[9] *See* https://www.gao.gov/assets/gao-07-737.pdf (June 2007) at 29.

black market."[10]

75. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police or other emergency medical services. An individual may not know that their driver's license was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud, or until the individual attempts to lawfully apply for unemployment and is denied benefits (due to the prior, fraudulent application and award of benefits).

G. Defendant's Conduct Violates HIPAA and Evidences Its Insufficient Data Security.

76. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of sensitive patient health information.

77. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

78. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII/PHI like the data Defendant left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.304, 45 C.F.R. § 164.306(a)(1-4), 45 C.F.R. § 164.312(a)(1),

[10] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Apr. 7, 2021).

45 C.F.R. § 164.308(a)(1)(i), 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

79. A Data Breach such as the one Defendant experienced, is considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as, "the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI ." See 45 C.F.R. 164.40

80. Defendant's Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations.

H. Plaintiff's and Class Members' Damages

81. Defendant has failed to provide any compensation for the unauthorized release and disclosure of Plaintiff's and the Class's PII/PHI other than offering twelve (12) months of complimentary credit-monitoring services to individuals involved in the Data Breach.

82. Plaintiff and the Class have been damaged by the compromise of their PII/PHI in the Data Breach.

83. Plaintiff and the Class presently face substantial risk of out-of-pocket fraud losses such as loans opened in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

84. Plaintiff and the Class have been, and currently face substantial risk of being targeted now and in the future, to PII/PHI phishing, data intrusion, and other illegality based on their PII/PHI being compromised in the Data Breach as potential fraudsters could use the information garnered to target such schemes more effectively against Plaintiff and the Class.

85. Plaintiff and the Class may also incur out-of-pocket costs for implementing protective measures such as purchasing credit monitoring fees, credit report fees, credit freeze fees, and other similar costs directly or indirectly related to the Data Breach.

86. Plaintiff and the Class also suffered a loss of value of their PII/PHI when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in data breach cases.

87. Plaintiff and the Class have spent and will continue to spend significant amounts of uncompensated time to monitor their financial accounts, medical accounts, sensitive information, credit score, and records for misuse.

88. Plaintiff and the Class have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

89. Moreover, Plaintiff and the Class have an interest in ensuring that their PII/PHI, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of proper and adequate security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing personal and financial information is not accessible online and that access to such data is password protected.

90. Further, as a result of Defendant's conduct, Plaintiff and the Class are forced to live with the anxiety and fear that their PII/PHI—which contains the most intimate details about a person's life—may be disclosed to the entire world, whether physically or virtually, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

91. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and the Class have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm because of the Data Breach.

I. Plaintiff's Experience

92. Plaintiff Melanie Burns entrusted her PII/PHI and other confidential information to

Defendant with the reasonable expectation and understanding that Defendant or its agents, would take industry-standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify her of any data security incidents related to her PII/PHI. Plaintiff would not have allowed Defendant's financial services to collect and maintain her PII/PHI had she known that Defendant would not take reasonable steps to safeguard her PII/PHI.

93. Plaintiff Burns has been forced to spend time dealing with and responding to the direct consequences of the Data Breach, which include spending time on telephone calls, researching the Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring her accounts. This is uncompensated time that has been lost forever and cannot be recaptured.

94. Plaintiff stores all documents containing her PII/PHI in a safe and secure location. Moreover, she diligently chooses unique usernames and passwords for the online accounts that she has.

95. Plaintiff has suffered actual injury in the form of damages to and diminution of the value of her PII/PHI – a form of intangible property that Plaintiff entrusted to Defendant. This PII/PHI was compromised in, and has been diminished as a result of, the Data Breach.

96. Plaintiff has also suffered actual injury in the forms of lost time and opportunity costs, annoyance, interference, and inconvenience as a result of the Data Breach, and has anxiety and increased concerns due to the loss of her privacy and the substantial risk of fraud and identity theft which she now faces.

97. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of her PII/PHI resulting from the compromise of

her PII/PHI in combination with her name, which is now in the hands of cyber criminals and other unauthorized third parties.

98. Knowing that thieves stole her PII/PHI and knowing that her PII/PHI will likely be sold on the dark web, has caused Plaintiff great anxiety.

99. Additionally, Plaintiff does not recall having been involved in any other data breaches in which her sensitive and confidential PII/PHI was compromised.

100. Plaintiff has a continuing interest in ensuring that her PII/PHI which, upon information and belief, remains in the possession of Defendant, is protected and safeguarded from future data breaches.

101. As a result of the Data Breach, Plaintiff is presently and will continue to be at a present and heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

V. CLASS ACTION ALLEGATIONS

102. Plaintiff brings this nationwide class action according to Federal Rules of Civil Procedure, Rules 23(b)(2), 23(b)(3), and 23(c)(4).

103. The nationwide Class that Plaintiff seeks to represent is defined as follows:

> All persons residing in the United States whose PII/PHI was compromised during the Data Breach that is the subject of the Notice of Data Breach published by Defendant on or about December 29, 2023 (the "Class").

104. Excluded from the Class are: (i) Defendant and its employees, officers, directors, affiliates, parents, subsidiaries, and any entity in which Defendant has a whole or partial ownership of financial interest; (ii) all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; (iii) any counsel and their respective staff appearing in this matter; and (iv) all judges assigned to hear any aspect of this litigation, their

immediate family members, and their respective court staff.

105. Plaintiff reserves the right to modify or amend the definitions of the proposed Class before the Court determines whether certification is appropriate.

106. **Numerosity**. The Class is so numerous that joinder of all members is impracticable. The Class includes thousands of individuals whose personal data was compromised by the Data Breach. The exact number of Class members is in the possession and control of Defendant and will be ascertainable through discovery. But, upon information and belief, the number of affected individuals exceeds 1,000.

107. **Commonality.** There are numerous questions of law and fact common to Plaintiff and the Class that predominate over any questions that may affect only individual Class members, including, without limitation:

a. Whether Defendant unlawfully maintained, lost or disclosed Plaintiff's and the Class's PII/PHI;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class to safeguard their PII/PHI;

f. Whether Defendant breached duties to Class to safeguard their PII/PHI;

g. Whether cyber criminals obtained Class's PII/PHI in the Data Breach;

h. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

i. Whether Defendant owed a duty to provide Plaintiff and Class timely notice of this Data Breach, and whether Defendant breached that duty;

j. Whether Plaintiff and Class suffered legally cognizable damages as a result of Defendant's misconduct;

k. Whether Defendant's conduct was negligent;

l. Whether Defendant's conduct violated federal law;

m. Whether Defendant's conduct violated state law; and

n. Whether Plaintiff and Class are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

108. **Typicality**. Plaintiff's claims are atypical of the claims of the Class in that Plaintiff, like all proposed Class members, had her PII/PHI compromised, breached, or otherwise stolen in the Data Breach. Plaintiff and the Class were injured through the uniform misconduct of Defendant, described throughout this Complaint, and assert the same claims for relief.

109. **Adequacy**. Plaintiff and counsel will fairly and adequately protect the interests of Plaintiff and the proposed Class. Plaintiff retained counsel who are experienced in Class action and complex litigation, particularly those involving Data Breach as is at issue in this class action complaint. Plaintiff has no interests that are antagonistic to, or in conflict with, the interests of other Class members.

110. **Superiority.** A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Moreover, absent a class action,

most Class members would find the cost of litigating their claims prohibitively high and would therefore have no effective remedy, so that in the absence of class treatment, Defendant's violations of law inflicting substantial damages in the aggregate would go unremedied without certification of the Class. Plaintiff and the Class have been harmed by Defendant's wrongful conduct and/or action. Litigating this action as a class action will reduce the possibility of repetitious litigation relating to Defendant's conduct and/or inaction. Plaintiff knows of no difficulties that would be encountered in this litigation that would preclude its maintenance as a class action.

111. Class certification is appropriate under Fed. R. Civ. P. 23(b)(1)(A), in that the prosecution of separate actions by the individual Class members would create a risk of inconsistent or varying adjudications with respect to individual members of the Class, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action conserves judicial resources and the parties' resources and protects the rights of each member of the Class. Specifically, injunctive relief could be entered in multiple cases, but the ordered relief may vary, causing Defendant to have to choose between differing means of upgrading its data security infrastructure and choosing the court order with which to comply. Class action status is also warranted because prosecution of separate actions by Class members would create the risk of adjudications with respect to individual Class members that, as a practical matter, would be dispositive of the interests of other members not parties to this action, or that would substantially impair or impede their ability to protect their interests.

112. Class certification, therefore, is appropriate under Rule 23(a) and (b)(2) because Defendant has acted or refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

113. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed its legal duty or obligation to Plaintiff and the Class to exercise due care in collecting, storing, using, safeguarding, or otherwise maintaining their PII/PHI;

b. Whether Defendant breached its legal duty to Plaintiff and the Class to exercise due care in collecting, storing, using, safeguarding, or otherwise maintaining their PII/PHI;

c. Whether Defendant failed to comply with its own policies or procedures and applicable laws, regulations, and industry standards relating to data security;

d. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach; and

e. Whether Plaintiff and the Class are entitled to actual damages, credit monitoring, or other injunctive relief, and/or punitive damages as a result of Defendant's wrongful conduct.

CAUSES OF ACTION

COUNT I

NEGLIGENCE

(On behalf of Plaintiffs and the Class)

114. Plaintiff and the Class re-allege and incorporate all foregoing paragraphs as if fully set forth herein.

115. Plaintiff and the Class entrusted Defendant with their PII/PHI.

116. Plaintiff and the Class entrusted their PII/PHI to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII/PHI for business purposes only, and not disclose their PII/PHI to unauthorized third parties.

117. Defendant owed a duty to Plaintiff and the Class to exercise reasonable care in obtaining, using, maintaining and protecting their PII/PHI from unauthorized third parties.

118. The legal duties owed by Defendant to Plaintiff and the Class include, but are not limited to the following:

a. To exercise reasonable care in procuring, retaining, securing, safeguarding, deleting, and protecting the PII/PHI of Plaintiff and the Class in Defendants possession;

b. To protect PII/PHI of Plaintiff and the Class in Defendants possession using reasonable and adequate security procedures that are compliant with industry-standard practices; and

c. To implement processes and software to quickly detect a data breach and to timely act on warnings about data breaches, including promptly notifying Plaintiff and Class of the Data Breach.

119. Defendant's duty to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45(a) (the "FTC Act"), which prohibits "unfair . . . practices in or affecting commerce," including, as interested and enforced by the Federal Trade Commission, the unfair practices by companies such as Defendant of failing to use

reasonable measures to protect PII/PHI.

120. Various FTC publications and data security breach orders further form the basis of Defendant's duty. Plaintiff and Class are consumers under the FTC Act. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII/PHI and by not complying with industry standards.

121. Defendant breached its duties to Plaintiff and the Class. Defendant knew or should have known the risks of collecting and storing PII/PHI and the importance of maintaining secure systems, especially in light of the fact that data breaches have recently been prevalent.

122. Defendant knew or should have known that its security practices did not adequately safeguard the PII/PHI of Plaintiff and the Class.

123. Through Defendant's acts and omissions described in this Complaint, including Defendant's failure to provide adequate security measures and its failure to protect the PII/PHI of Plaintiff and the Class from being foreseeably captured, accessed, exfiltrated, stolen, disclosed, and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the PII/PHI of Plaintiff and the Class during the period it was within Defendant's possession and control.

124. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential PII/PHI, a necessary part of obtaining services from Defendant.

125. Defendant was subject to an "independent duty" to Plaintiff and the class.

126. Defendant's own conduct created a foreseeable risk of harm to an individual, including Plaintiff and the Class. Defendant's misconduct included, but was not limited to, their

failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included their decisions not to comply with industry standards for safekeeping of the PII/PHI of Plaintiff and the Class, including basic encryption techniques freely available to Defendant.

127. Defendant was in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

128. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII/PHI of Plaintiff and the Class.

129. Defendant breached the duties it owes to Plaintiff and Class in several ways, including:

a. Failing to implement adequate security systems, protocols, and practices sufficient to protect Plaintiff and the Class's PII/PHI and thereby creating a foreseeable risk of harm;

b. Failing to comply with the minimum industry data security standards during the period of the Data Breach;

c. Failing to act despite knowing or having reason to know that its systems were vulnerable to attack; and

d. Failing to timely and accurately disclose to Plaintiff and the Class that their PII/PHI had been improperly acquired or accessed and was potentially available for sale to criminals on the dark web.

130. There is a close causal connection between Defendant's failure to implement security measures to protect the PII/PHI of Plaintiff and Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Class. The PII/PHI of Plaintiff and the Class was stolen and

accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII/PHI by adopting, implementing, and maintaining appropriate security measures.

131. Due to Defendant's misconduct, Plaintiff and the Class are entitled to credit monitoring at a minimum. The PII/PHI taken in the Data Breach can be used for identity theft and other types of financial fraud against Plaintiff and the Class.

132. Some experts recommend that data breach victims obtain credit monitoring services for at least ten years following a data breach. Annual subscriptions for credit monitoring plans range from approximately $219 to $358 per year. To date, Defendant has only offered twelve (12) months of complimentary credit-monitoring services.[11]

133. As a result of Defendant's negligence, Plaintiff and Class suffered injuries that include:

i. the lost or diminished value of PII/PHI;

ii. out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII/PHI;

iii. lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including, but not limited to, time spent deleting PII/PHI shing email messages and cancelling credit cards believed to be associated with the compromised account;

iv. the continued risk to their PII/PHI, which may remain for sale on the dark web and is in Defendant's possession and subject to further unauthorized disclosures so long as Defendant fails to undertake

[11] *See n* 1.

appropriate and adequate measures to protect the PII/PHI in their continued possession;

v. future costs in terms of time, effort, and money that will be expended to prevent, monitor, detect, contest, and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class, including ongoing credit monitoring.

134. These injuries were reasonably foreseeable given the history and uptick of data security breaches of this nature within the financial and/or medical sector. The injury and harm that Plaintiff and the Class suffered was the direct and proximate result of Defendant's negligent conduct.

COUNT II

NEGLIGENCE *PER SE*

(On behalf of Plaintiff and the Class)

135. Plaintiff and the Class re-allege and incorporate all foregoing paragraphs as if fully set forth herein.

136. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII/PHI. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

137. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII/PHI and comply with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII/PHI it obtained and stored and the foreseeable harm.

138. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII/PHI like the data Defendant left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.304, 45 C.F.R. § 164.306(a)(1-4), 45 C.F.R. § 164.312(a)(1), 45 C.F.R. § 164.308(a)(1)(i), 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

139. Defendant's violations of Section 5 of the FTC Act and HIPAA constitute negligence *per se*.

140. Plaintiff and the Class are within the class of persons that the FTCA and HIPAA were intended to protect.

141. The harm that occurred as a result of the Data Breach is the type of harm the FTCA and HIPAA were intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

142. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) actual instances of identity theft or fraud; (ii) the compromise, publication, and/or theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud, identity theft; and/or other various forms of

fraud (v) costs associated with placing or removing freezes on credit reports; (vi) the continued risk to their PII/PHI, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII/PHI of Plaintiff and the Class in its continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII/PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class.

143. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII/PHI, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII/PHI in its continued possession.

144. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT III

UNJUST ENRICHMENT

(On behalf of Plaintiff and the Class)

145. Plaintiff and the Class re-allege and incorporate all foregoing paragraphs as if fully set forth herein.

146. Plaintiff and the Class conferred a monetary benefit to Defendant by providing Defendant with their valuable PII/PHI, which Defendant knowingly used or retained in the course of its business.

147. Defendant benefited from receiving Plaintiff's and the Class members' PII/PHI by

its ability to retain and use that information for its own financial business benefit. Defendant understood this benefit and accepted the benefit knowingly.

148. Defendant also understood and appreciated that the PII/PHI of Plaintiff and the Class was private and confidential to them, and that its value depended upon Defendant maintaining the privacy and confidentiality of that PII/PHI.

149. Plaintiff and the Class conferred a monetary benefit upon Defendant in the form of monies paid to Defendant for services.

150. The monies paid to Defendant for services involving Plaintiff and the Class PII/PHI were to be used by Defendant, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

151. Defendant also understood that Plaintiff's and the Class's PII/PHI was private and confidential, and its value depended upon Defendant maintaining the privacy and confidentiality of that PII/PHI.

152. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid their data security obligations at the expense of Plaintiff and the Class by utilizing cheaper, ineffective security measures. Plaintiff and the Class, on the other hand, suffered a direct and proximate result of Defendant's failure to provide the requisite security.

153. But for Defendant's willingness and commitment to maintain privacy and confidentiality, that PII/PHI would not have been transferred to and entrusted with Defendant. Indeed, if Defendant had informed its customers that Defendant's data and cyber security measures were inadequate, Defendant would not have been permitted to continue to operate in that fashion by regulators, its shareholders, and its consumers.

154. As a result of Defendant's wrongful conduct, Defendant has been unjustly enriched at the expense of, and to the detriment of, Plaintiff and the Class. Defendant continues to benefit and profit from their retention and use of the PII/PHI while its value to Plaintiff and the Class has been diminished.

155. Defendant's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged in this complaint, including compiling, using, and retaining Plaintiff and the Class's PII/PHI, while at the same time failing to maintain that information securely from intrusion and theft by cyber criminals, hackers, and identity thieves.

156. Plaintiff and the Class have no adequate remedy at law.

157. Under principals of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and the Class because Defendant failed to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiff and the Class paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

158. Defendant acquired the monetary benefit and PII/PHI through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

159. As a direct and proximate result of Defendant's conduct, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and the Class, proceeds that they unjustly received from them.

160. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class have suffered, and will continue to suffer, ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss an economic

harm; actual identify theft crimes, fraud, and abuse resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic time that the Plaintiff and Class have not been compensated for.

161. As a direct and proximate result of Defendant's conduct, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm.

COUNT IV

BREACH OF IMPLIED CONTRACT

(On behalf of Plaintiff and the Class)

162. Plaintiff and the Class re-alleges and incorporates all foregoing paragraphs as if fully set forth herein.

163. Plaintiff and the Class entrusted their PII/PHI with Defendant. In doing so, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached, compromised, or stolen.

164. The statements in Defendant's Privacy Policy described herein support the existence of an implied contract.

165. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant.

166. Defendant breached the implied contract with Plaintiff and the Class by failing to safeguard and protect their PII/PHI, by failing to delete the PII/PHI of Plaintiff and the Class once

their relationship ended, and by failing to provide timely and accurate notice to them that the PII/PHI was compromised as a result of the Data Breach.

167. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class have suffered, and will continue to suffer, ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss an economic harm; actual identify theft crimes, fraud, and abuse resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic time that the Plaintiff and Class have not been compensated for.

168. As a direct and proximate result of the Defendant's above-described breach of implied contract, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT V

BREACH OF FIDUCIARY DUTY

(On behalf of Plaintiff and the Class)

169. Plaintiff and the Class re-allege and incorporate all foregoing paragraphs as if fully set forth herein.

170. Defendant became a fiduciary by its undertaking and guardianship of the PII/PHI, to act primarily for Plaintiff and Class Members, (1) for the safeguarding of Plaintiff and Class Members' PII/PHI; (2) to timely notify Plaintiff and the Class of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and

does store.

171. Defendant has a fiduciary duty to act for the benefit of Plaintiff and the Class upon matters within the scope of Defendant's relationship with its patients, in particular, to keep secure their PII/PHI.

172. Defendant breached its fiduciary duties to Plaintiff and the Class by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

173. Defendant breached its fiduciary duties to Plaintiff and the Class by failing to encrypt or otherwise protect the integrity of the systems containing Plaintiff and the Class's PII/PHI.

174. Defendant breached its fiduciary duties owed to Plaintiff and the Class by failing to timely notify and/or warn Plaintiff and the Class of the Data Breach.

175. Defendant breached its fiduciary duties to Plaintiff and the Class by failing to otherwise safeguard Plaintiff and the Class's PII/PHI.

176. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class have suffered, and will continue to suffer, ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identify theft crimes, fraud, and abuse resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic time that the Plaintiff and Class have not been compensated for.

177. As a direct and proximate result of Defendant's breach of fiduciary duties, Plaintiff

and Class have suffered and will continue to suffer other forms of injury and/or harm, and economic and non-economic losses.

COUNT VI

BREACH OF THE IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING

(On behalf of Plaintiff and the Class)

178. Plaintiff and the Class re-allege and incorporate all foregoing paragraphs as if fully set forth herein.

179. Every contract in this state has an implied covenant of good faith and fair dealing. This implied covenant is an independent duty and may be breached even when there is no breach of a contract's express terms.

180. In addition, there exists an implied covenant of good faith and fair dealing in all contracts that neither party shall do anything which will have the effect of destroying or injuring the right of the other party to receive the fruits of the contract. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit – not merely the letter – of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form. Evading the spirit of the bargain and abusing the power to specify terms constitute examples of bad faith in the performance of contracts.

181. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty. Examples of bad faith are evasion of the spirit of the bargain, willful rendering of imperfect performance, abuse of a power to specify terms, and interference with or failure to cooperate in the other party's performance.

182. Plaintiff and the class have complied with and performed all conditions of their contracts with Defendant.

183. Defendant breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard Plaintiff and Class Members' PII/PHI, failing to timely and accurately disclose the Data Breach to Plaintiffs and Class Members and continued acceptance of PII/PHI and storage of other personal information after Defendant knew, or should have known, of the security's vulnerabilities of the systems that were exploited in the Data Breach.

184. Defendant acted in bad faith and/or with malicious motive in denying Plaintiff and Class Members the full benefit of their bargains as originally intended by the parties, thereby causing them injury in an amount to be determined at trial.

COUNT VII

DECLARATORY JUDGMENT AND INJUNCTIVE RELIEF

(On behalf of Plaintiff and the Class)

185. Plaintiff and the Class re-allege and incorporate all foregoing paragraphs as if fully set forth herein.

186. Plaintiff pursues this claim under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

187. Defendant owes a duty of care to Plaintiff and the Class that requires it to adequately secure Plaintiff's and the Class's PII/PHI.

188. Defendant failed to fulfill their duty of care to safeguard Plaintiff's and Class's PII/PHI.

189. Plaintiff and the Class are at risk of harm due to the exposure of their PII/PHI and

Defendant's failure to address the security failings that lead to such exposure.

190. Plaintiff, therefore, seeks a declaration that (1) Defendant's existing security measures do not comply with their explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices appropriate to the nature of the information to protect customers' personal information, and (2) to comply with their explicit or implicit contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. Engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Engaging third-party security auditors and internal personnel to run automated security monitoring;

c. Auditing, testing, and training its security personnel regarding any new or modified procedures;

d. Segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. Conducting regular database scanning and security checks;

f. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a

breach;

g. Purchasing credit monitoring services for Plaintiff and the Class for a period of ten years; and

h. Meaningfully educating Plaintiff and the Class about the threats they face as a result of the loss of their PII/PHI to third parties, as well as the steps they must take to protect themselves.

VI. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and all others similarly situated, requests judgment against Defendant and that the Court grant the following:

1. For an order certifying the Class and appointing Plaintiff and her counsel to represent the Class;

2. For an order enjoining Defendant from engaging in the wrongful conduct alleged herein concerning disclosure and inadequate protection of the PII/PHI belonging to Plaintiff and the Class;

3. For injunctive relief requiring Defendant to:

   a. Engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

   b. Engage third-party security auditors and internal personnel to run automated security monitoring;

   c. Audit, test, and train its security personnel regarding any new or

modified procedures;

d. Segment their user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. Conduct regular database scanning and security checks;

f. Routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

g. Purchase credit monitoring services for Plaintiff and the Class for a period of ten years; and

h. Meaningfully educate Plaintiff and the Class about the threats they face as a result of the loss of their PII/PHI to third parties, as well as the steps they must take to protect themselves.

4. An order instructing Defendant to purchase or provide funds for credit monitoring services for Plaintiff and all Class members;

5. An award of compensatory, statutory, nominal and punitive damages, in an amount to be determined at trial;

6. An award for equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

7. An award of reasonable attorneys' fees, costs, and litigation expenses, as allowable by law; and

8. Any and all such other and further relief as this Court may deem just and proper.

VII. DEMAND FOR JURY TRIAL

Plaintiff hereby demands this matter be tried before a jury.

Respectfully submitted,

Dated: January 8, 2024

/s/ Tiffany Marko Yiatras

Tiffany Marko Yiatras, #58197MO
Francis J. "Casey" Flynn, Jr.
CONSUMER PROTECTION LEGAL, LLC
308 Hutchinson Road
Ellisville, Missouri 63011-2029
Tele: 314-541-0317
Email: tiffany@consumerprotectionlegal.com
Email: casey@consumerprotectionlegal.com

William B. Federman (pro hac vice forthcoming)
FEDERMAN & SHERWOOD
10205 North Pennsylvania Avenue
Oklahoma City, OK 73120
Telephone: (405) 235-1560
-and-
212 W. Spring Valley Road
Richardson, TX 75081
wbf@federmanlaw.com

Attorneys for Plaintiff and Putative Class
**Pro Hac Vice forthcoming*